UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,065	07/08/2003	Sung-Ming Yen	HUS91229/PI	8008

23616   7590   09/28/2006

LAW OFFICES OF CLEMENT CHENG
17220 NEWHOPE STREET #127
FOUNTAIN VALLEY, CA 92708

EXAMINER
SHAN, APRIL YING

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*08 July 2003*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☒ All   b)☐ Some * c)☐ None of:

　　　　1.☒ Certified copies of the priority documents have been received.

　　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>*08 July 2003*</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-11 have been examined.

Priority

2.   Acknowledgment is made of Applicant's claim for foreign priority based on an application filed in Taiwan on 27 December 2002. It is noted, however, that applicant has not field a certified copy of the 091137721 application as required by 35 U.S.C. 119(b).

3.   Should applicant desire to obtain the benefit of foreign priority under 35 U.S.C. 119(a)-(d) prior to declaration of an interference, a translation of the foreign application should be submitted under 37 CFR 1.55 in reply to this action.

Drawings

4.   The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the algorithm comprising the steps of in claim 1, lines 16-24 on page 18 and line 1 on page 19 must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate

prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5.   The disclosure is objected to because of the following informalities:

For example,

a.   Page 9, line 16, "from both C safe-error attack" should be "from C safe-error attack;

b.   Page 10, line 22, "a one" should be "one";

Check the specification and correct any informality the Applicant is aware of.

Claim Objections

6.   Claims 1-11 are objected to because of the following informalities:

For example,

    a.   In claim 1, line 11, "as a one" should be "as one";

    b.   In claim 5, line 22, "crypotographic" should be "cryptographic";

    c.   In claim 8, line 14, "as a one" should be "as one";

    d.   Any claim not specifically addressed, above, is being objected as

incorporating the deficiencies of a claim upon which it depends.

Appropriate correction is required.

    Check the claims 1-11 and correct any informality the Applicant is aware of.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7.   Claims 1-11 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

    Claim 1 recites the limitations "a fourth bit" is recited in line 17. Since there are

no first bit, second bit or a third bit in the claim, "a fourth bit" is undefined. Additionally,

"said fourth value" recited in lines 22 and 24 lacks of an antecedent basis for this

limitation in the claim.

Claim 5 recites the limitations "a fourth bit" is recited in line 3, page 20. Since there are no first bit, second bit or a third bit in the claim, "a fourth bit" is undefined. Additionally, "said fourth value" recited in lines 11 and 16 lacks of an antecedent basis for this limitation in the claim.

Claim 8 recites the limitations "a fourth bit" is recited in line 3, page 20. Since there are no first bit, second bit or a third bit in the claim, "a fourth bit" is undefined. Additionally, "said fourth value" recited in lines 25 and 26 lacks of an antecedent basis for this limitation in the claim.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 101

8.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9.   Claims 1-11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-4 are directed to a method for protecting public key schemes. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. The claimed steps do not result in a tangible result. Claims 1-4 are rejected as being directed to an abstract idea (i.e., producing non-tangible result) [tangible requirement does require that the claim must recite more

than a 101 judicial exception, in that the process must set forth a practical application of

that 101 judicial exception to produce a real-world result, Benson, 409 U.S. at 71-72,

175 USPQ at 676-77).

Claims 5-7 are directed to an apparatus for protecting public key schemes.

However, it appears that the apparatus would reasonably be interpreted by one of

ordinary skill in the art as software, per se. There is no element positively recited as

part of the apparatus. Applicant's specification provides no explicit and deliberate

definition on any element positively recited as part of the apparatus, and it appears that

such would reasonably be interpreted as representative of the software which protects

public key schemes from timing, power monitoring and fault attacks. As such, it

believed that the apparatus of claim 5-7 is reasonably interpreted as functional

descriptive material, per se.

Claims 8-11 are directed to a computer-readable medium for protecting public

key schemes. The examiner respectfully asserts that the claimed subject matter does

not fall within the statutory classes listed in 35 USC 101. The claimed logic code does

not result in a tangible result. Claims 8-11 are rejected as being directed to an abstract

idea (i.e., producing non-tangible result) [tangible requirement does require that the

claim must recite more than a 101 judicial exception, in that the process must set forth a

practical application of that 101 judicial exception to produce a real-world result,

Benson, 409 U.S. at 71-72, 175 USPQ at 676-77).

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

11.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

    1.   Determining the scope and contents of the prior art.
    2.   Ascertaining the differences between the prior art and the claims at issue.
    3.   Resolving the level of ordinary skill in the pertinent art.
    4.   Considering objective evidence present in the application indicating
           obviousness or nonobviousness.

12.   This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

13.   Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Kocher et al. (U.S. Patent 6,298,442) in view of Benoit (WO/2001/055838) (English

translation is provided by US Pub. No. 2003/0053621 and the rejections below refer to the English translation)

As per **claim 1**, Kocher et al. discloses a method for protecting public key schemes from timing, power monitoring and fault attacks comprising the steps of: obtaining a message for use in a cryptographic operation (obtaining a base representative of at least a portion of said message – e.g. claim 18/a); obtaining a modulus and an exponent corresponding to said cryptographic operation (claim 18/a), wherein said exponent contains at least one bit (y is the exponent of k bits in length – e.g. col. 4, line 17); initializing a first value as a one (R=1 in step 100 of fig. 1), executing a modulo exponentiation algorithm on each bit of said exponent from the most significant bit to the least significant bit (col. 4, lines 19-27 and col. 5, lines 63-67) wherein said algorithm comprising the steps of:

input a bit to an inverter and storing the output as a third value, and assigning the next bit of said bit as a fourth bit (col. 6, lines 12-19); if said third value is a zero, updating said first value with the result of squaring, modulo said modulus said first value, if said third value is a one, updating said first value with the result of multiplying, modulo said modulus said first value by said second value (col. 7, lines 57-60, claims 19/a, 19/b and col. 7, lines 18-23); and if said fourth value is a zero, updating said first value with the result of squaring, modulo said modulus said first value, if said

fourth value is a one, updating said first value with the result of multiplying, modulo said modulus said first value by said second value (col. 7, lines 57-60, claims 19/a, 19/b and col. 7, lines 18-23); updating said bit with the next bit of said bit (The exponent bit position is updated whenever the processing moves to a new exponent bit – e.g. col. 6, lines 45-46), and executing steps of said algorithm on said bit until said bit being said least significant bit of said exponent (Finally, the value is subtracted from I, which has the effect of decrementing I if the least significant bit of v is set. At step 145, the device determines whether the exponentiation has completed. If I is less than zero, processing continues to step 160 – e.g. col. 6, lines 38-43); and storing and output said first value (Return (R) – e.g. col. 4, lines 25).

The difference between the claimed invention and that disclosed in Kocher et al. is the latter does not disclose the claimed feature of assigning said message to a second value. However, such missing feature in Kocher et al. is clearly taught in paragraph [0062] aforementioned Benoit reference, the same field endeavor. It would have been obvious for a person having ordinary skill in the art to incorporate such well known feature as taught in the Benoit reference into the Kocher et al. method motivated by adding "this makes it possible to indicate in which register the correct result is situated" (Benoit, paragraph [0062])

As per **claims 2 and 4**, combination of Kocher et al. and Benoit disclose a method as applied in claim 1. Kocher et al. further discloses wherein if said bit is said least significant bit of said exponent, said fourth value is initialized as 1 (step 100 of fig. 1) and wherein said inverter is used for output a one if input a zero into it, and output a zero if input a one into it (col. 5, lines 48-50 and col. 6, lines 16-17)

As per **claim 3**, combination of Kocher et al. and Benoit discloses a method as applied in claim 2. Kocher et al. further discloses wherein said bit is one bit of bits of said exponent and is a one or a zero (col. 4, lines 40-42).

As per **claim 5**, Kocher et al. discloses an apparatus for protecting public key schemes from timing, power monitoring and fault attacks comprising:

means for obtaining a message for use in a cryptographic operation (This process is performed by a general purpose microprocessor, by a dedicated cryptogrocessor, or by some other underlying processor, in accordance with software and/or hardwired instructions –e.g. col. 5, lines 39-43);

means for obtaining a modulus and an exponent corresponding to said crypotographic operation, wherein said exponent contains at least

one bit; means for initializing a first value as a one, and assigning said message to a second value; means for executing a modulo exponentiation algorithm on each bit of said exponent from the most significant bit to the least significant bit, wherein said algorithm comprising: means for input a bit into an inverter and storing the output as a third value, and assigning the next bit of said bit as a fourth bit; means for determining whether said third value is a one or a zero; means for updating said first value with the result of squaring if said third value is a one, modulo said modulus said first value, updating said first value with the result of multiplying, modulo said modulus said first value by said second value if said third value is a one; means for determining whether said fourth value is a one or a zero; and means for updating said first value with the result of squaring, modulo said modulus said first value if said fourth value is a zero, updating said first value with the result of multiplying, modulo said modulus said first value by said second value if said fourth value is a one; means for updating said bit with the next bit of said bit, and executing steps of said algorithm on said bit until said bit being said least significant bit of said exponent; means for determining whether said bit is a one or a zero; and means for storing and output said first value (col. 5, lines 39-43 and col. 6, lines 1-3)

The difference between the claimed invention and that disclosed in Kocher et al. is the latter does not disclose the claimed feature of means

for assigning said message to a second value. However, such missing

feature in Kocher et al. is clearly taught in paragraph [0062]

aforementioned Benoit reference, the same field endeavor. It would have

been obvious for a person having ordinary skill in the art to incorporate

such well known feature as taught in the Benoit reference into the Kocher

et al. method motivated by adding "this makes it possible to indicate in

which register the correct result is situated" (Benoit, paragraph [0062])

As per **claims 6-7**, combination of Kocher et al. and Benoit

disclose an apparatus as applied in claim 5. Kocher et al. further

discloses wherein said bit is one bit of bits of said exponent and is a one

or a zero (col. 4, lines 40-42) and wherein said inverter is used for output a

one if input a zero into it, and output a zero if input a one into it (col. 6,

lines 12-19).

As per **claims 8-11**, combination of Kocher et al. and Benoit

disclose the claimed method of steps as applied above in claims 1-4.

Therefore, combination of Kocher et al. and Benoit disclose the claimed

logic code embodied in a computer readable medium for carrying out the

method of steps.

Conclusion

14.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

> Joye et al. (US 2005/0084096) discloses a method for implementing in an

   electronic component a cryptographic algorithm using calculating means.

> Joye et al. (US 2004/0184604) discloses a secure method for performing an

   exponentiation operation.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

19 September 2006
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100